National Vulnerability Database (NVD)

Information Security and Privacy Advisory Board
November 3-5, 2010

Chris Johnson
Computer Security Division
Information Technology Laboratory
The National Institute of Standards and Technology (NIST)

Agenda

- National Vulnerability Database (NVD) Overview
- NVD Components
- NVD Analysis Activities
- NVD Data Feeds
- National Checklist Program (NCP)
- Security Content Automation Protocol (SCAP) Resources

NVD Overview

- U.S. government repository of IT vulnerability information
- NVD database currently contains >44,000 vulnerability entries
- Website received over 40 million hits in CY 2009
- NVD data holdings are used extensively by government, industry and academia

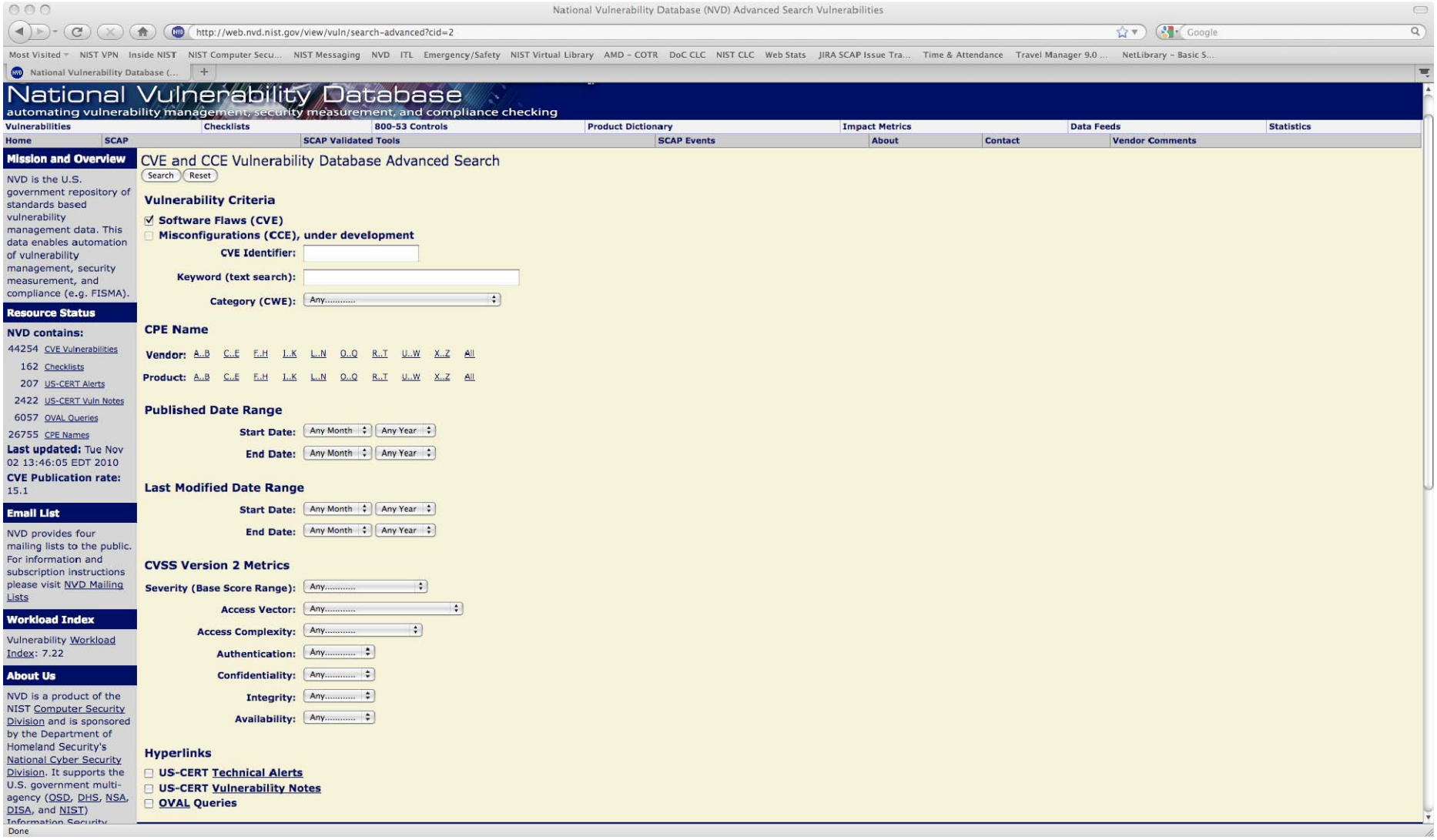
NVD Components

- National Vulnerability Database
  - Security-related software flaws
  - IT product dictionary
- National Checklist Program Website
  - Repository of low level checklists for securing operating systems and applications
- SCAP Validation Program Website
  - List of products that conform to the NIST-published SCAP validation requirements
- SCAP Resources
  - SCAP publications, data repositories and tools

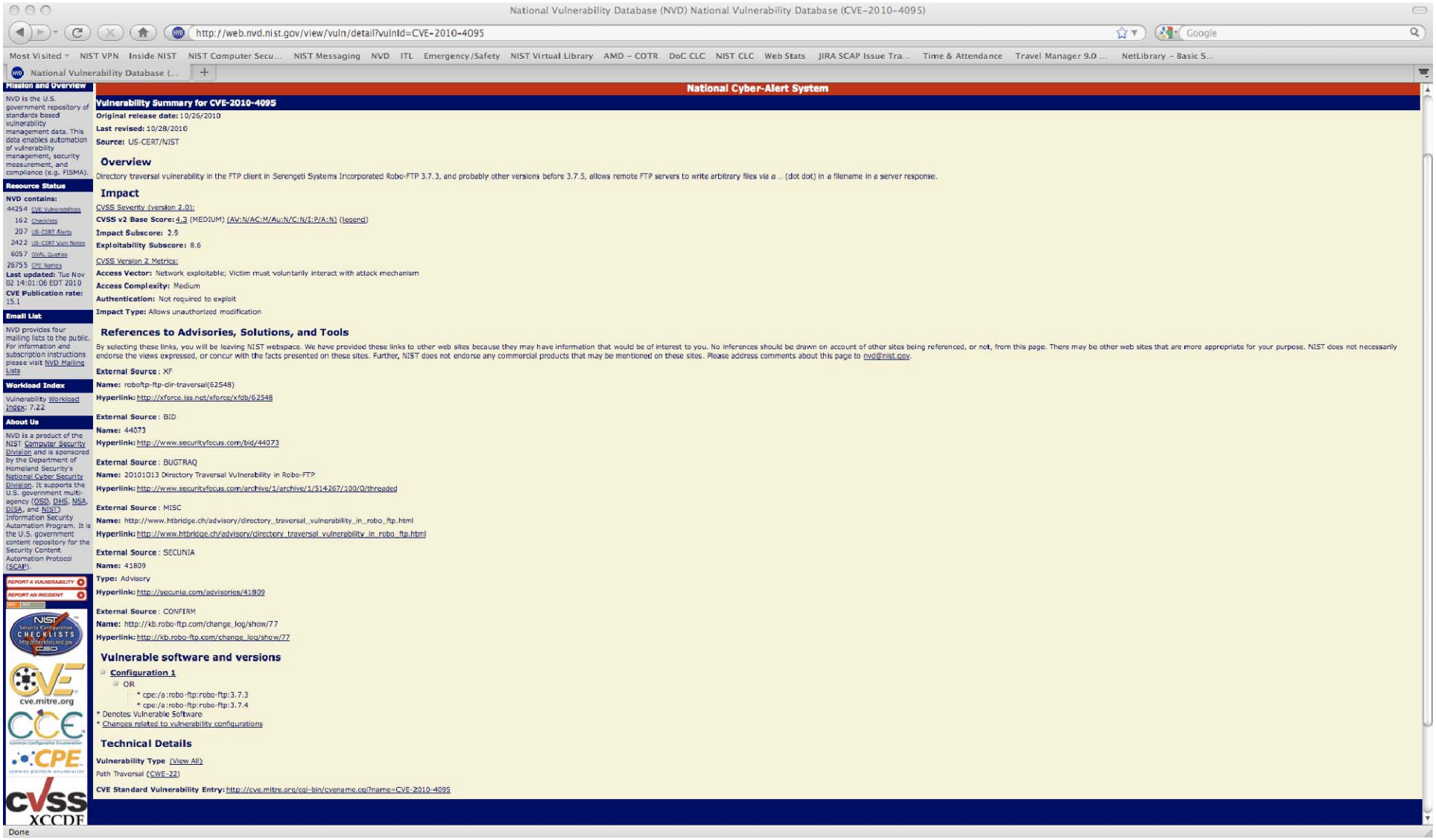
NVD Vulnerability Analysis Activities

- NVD contains over 44,000 Common Vulnerabilities and Exposures (CVE®) entries with the NVD Analysis Team analyzing ~6,000 vulnerabilities a year
  - Compute and publish impact metrics (i.e., Common Vulnerability Scoring System [CVSS] base scores)
  - Express affected platforms (e.g., software & versions) using a uniform naming convention – the Common Platform Enumeration
  - Describe the underlying weakness or root cause (e.g., buffer overflow, input validation error) of the software flaw using the Common Weakness Enumeration
  - Mediate vendor comments and community feedback

NVD Advanced Search Capabilities



NVD Vulnerability Summary



NVD Data Feeds

- Machine-readable vulnerability data feeds
  - >23,000 downloads of the NVD vulnerability data feeds in July 2010
- Product dictionary containing over 26,000 unique product names
  - 992 downloads of the NVD CPE dictionary file in July 2010
- Spanish language vulnerability data feeds (translations performed by INTECO personnel)
- Beta Common Configuration Enumeration (CCE) to 800-53 mappings

National Checklist Program (NCP)

- NCP website contains 162 low-level checklists that are categorized as follows:
  - Tier I – Prose checklists
  - Tier II – Non-SCAP automated content
  - Tier III – Designed to work in an SCAP-validated tool
  - Tier IV – Will work in an SCAP-validated tool
- Checklist submissions come from a variety of organizations – government agencies, software vendors and third parties
- Submission guidelines for the NCP are described in NIST Special Publication 800-70, Rev. 1; National Checklist Program for IT Products-Guidelines for Checklist Users and Developers

SCAP Resources

- SCAP Publications
  - NIST SP 800-117: Guide to Adopting and Using the Security Content Automation Protocol
  - NIST SP 800-126: The Technical Specification for the Security Content Automation Protocol
  - NIST IR 7511: Security Content Automation Protocol (SCAP) Validation Program Test Requirements
- SCAP Content Development Tools
  - Enhanced SCAP Editor (eSCAPe)
  - Recommendation Tracker
  - SCAP Content Validation Tool

SCAP Validation Program Website

- List of products that have been validated by NIST as conforming to the SCAP and its component specifications
- Full description of SCAP product validation information, capabilities and status
- 40 SCAP validated products from 30 product vendors
- 9 National Voluntary Laboratory Accreditation Program (NVLAP) Accredited Independent SCAP Testing Laboratories

NVD Future Capabilities

- Create a CCE analysis and scoring capability based on the Common Configuration Scoring System (CCSS)
- Design, build and implement web services that handle requests for NVD SCAP data products.
- Develop and deploy web services & interactive web portal that will streamline and expedite the NCP checklist submission process and help ensure the completeness of submission packages

Questions?

Contact Info

Christopher Johnson

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

christopher.johnson@nist.gov

(301) 975-5981

National Vulnerability Database

http://nvd.nist.gov